Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.7.1 Цифровая форензика»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.В.Э.7.1 Цифровая форензика*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 9 от "20" марта 2026 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:

должность *подпись* Ю.Д. Фот *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
С.А. Биктимирова
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Фот Ю.Д., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Сформировать у студентов системные знания и практические навыки по обнаружению, фиксации, изъятию, исследованию и документированию цифровых доказательств в соответствии с принципами юридической достоверности и сохранения целостности данных.

Задачи:

1. *Освоить правовые и процедурные основы цифровой форензики.*
2. *Научиться создавать криминалистически корректные образы дисков и памяти.*
3. *Изучить методы анализа файловых систем, логов, реестра и оперативной памяти.*
4. *Приобрести навыки восстановления удалённых данных и фрагментированных файлов.*
5. *Научиться формировать экспертные заключения и временные шкалы событий.*

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.28 Основы информационной безопасности*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-2 Формирование требований в защите информации в автоматизированных системах	ПК*-2-В-1 Умеет определять угрозы безопасности информации, обрабатываемой автоматизированной системой ПК*-2-В-2 Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации ПК*-2-В-3 Владеет навыками разработки архитектуры системы защиты информации автоматизированной системы	**Знать:** Нормативно-правовую базу (ФСТЭК, приказы Минцифры, УПК РФ) в части требований к обеспечению возможности расследования инцидентов в АС. Типовые артефакты цифровой форензики (логи, MFT, реестр, дампы памяти) и их роль в формировании требований к аудиту, регистрации событий и сохранению доказательств. Методы и инструменты для верификации выполнения требований

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		ЗИ через анализ образов дисков и дампов памяти. Принципы построения временных шкал (timeline) и их использование для обоснования требований к синхронизации времени и неизменности логов в АС. Критерии допустимости и целостности цифровых доказательств, влияющие на требования к защите от модификации и удаления журналов событий. Особенности формирования требований для различных типов АС (Windows, Linux, мобильные, встраиваемые) с учётом возможностей последующей форензики. **Уметь:** Анализировать существующие средства аудита и регистрации событий в АС с позиции их пригодности для цифровой форензики. Формулировать требования к логированию (какие события, куда, с какой детализацией, на какой срок хранения) на основе типовых сценариев расследования. Обосновывать необходимость включения в требования ЗИ механизмов криптографической защиты целостности логов и дампов памяти. Проводить оценку полноты и непротиворечивости требований к защите информации с помощью форензических

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		инструментов (например, проверить, фиксируется ли удаление файлов через аудит). Разрабатывать требования к изоляции процессов, контейнеризации и виртуализации, исходя из необходимости сохранения доказательной базы при инциденте. Составлять разделы технического задания на АС в части подсистемы анализа инцидентов и форензической готовности **Владеть:** Методикой аудита соответствия АС требованиям ЗИ с использованием форензических инструментов. Навыком разработки шаблонов требований к журналам событий, цепочке хранения доказательств и временной синхронизации. Приёмами верификации требований к защите от удаления и модификации логов (например, проверка неизменяемости журналов через анализ файловой системы). Способностью формировать рекомендации по доработке АС на основе выявленных форензическим анализом недостатков (отсутствие аудита, короткий срок хранения, слабая защита ключей). Навыком интеграции форензических требований в жизненный

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		цикл АС (на этапах проектирования, ввода в эксплуатацию, сопровождения).

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**68,25**	**68,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- написание реферата;* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к зачету.*	**39,75**	**39,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основы цифровой форензики: правовые и процедурные аспекты	30	10		10	10
2	Инструментальный анализ носителей и оперативной памяти	39	12		12	15
3	Артефакты операционных систем, временные шкалы и экспертная деятельность	39	12		12	15
	Итого:	108	34		34	40
	Всего:	108	34		34	40

4.2 Содержание разделов дисциплины

Раздел 1. Основы цифровой форензики: правовые и процедурные аспекты
Лекция 1. Введение в цифровую форензику

1. Определение цифровой форензики, её цели и задачи.
2. Место форензики в информационной безопасности и в уголовном процессе.
3. Виды форензики: компьютерная, мобильная, сетевая, облачная, IoT.
4. Основные принципы работы с цифровыми доказательствами (неизменность, цепочка хранения, обоснованность).
5. Международные стандарты: ISO/IEC 27037, NIST SP 800-86, ACPO (Великобритания).
6. Жизненный цикл цифрового доказательства от изъятия до суда.
7. Роль эксперта-криминалиста, требования к квалификации.
8. Типичные ошибки начинающих экспертов (изменение метаданных, работа на live-системе).

Лекция 2. Правовые аспекты и цепочка хранения доказательств

1. Правовая база РФ: УПК, ФЗ «Об информации», приказы ФСТЭК России.
2. Критерии допустимости и относимости цифровых доказательств.
3. Понятие «целостность доказательств» в юридическом смысле.
4. Журнал передачи носителей: обязательные поля, подписи, временные метки.
5. Пломбирование, опечатывание и видеозапись процедур.
6. Постановление о назначении экспертизы, вопросы эксперту.
7. Структура заключения эксперта (вводная, исследовательская, выводы).
8. Особенности работы с адвокатом и в судебном заседании.

Лекция 3. Основы анализа файловых систем (FAT32, NTFS, ext4)

1. Структура загрузочного сектора MBR и GPT.
2. Организация данных в FAT32: таблица FAT, корневой каталог.
3. NTFS: MFT (Master File Table), атрибуты (стандартные, данные, $INDEX_ROOT).
4. Альтернативные потоки данных NTFS (ADS) и их форензическое значение.
5. Журналирование в NTFS ($LogFile) и ext4 (журнал).
6. Временные метки MACB (Modified, Accessed, Changed, Born).
7. Различия в удалении файлов в FAT, NTFS, ext4.
8. Анализ битмапов и дескрипторов.

Лекция 4. Восстановление удалённых данных. Принципы карательной утилиты

1. Как операционная система помечает удалённые файлы (битмап, $MFT, inode).
2. Ручное восстановление по сигнатурам (магические заголовки, footer).
3. Влияние фрагментации на восстановление.
4. Риск перезаписи данных (TRIM, дефрагментация, работа ОС).
5. Обзор инструментов: Photorec, Foremost, Scalpel, Autopsy, Recuva.
6. Понятие «карательная утилита» (carving) — преимущества и недостатки.
7. Ложные срабатывания и методы их снижения.

Лекция 5. Инструментарий Windows для сбора данных и Sysinternals

1. Правила live-форензики (порядок сбора данных, риск изменения памяти).
2. Sysinternals Suite: назначение, лицензия, режимы запуска.
3. Process Explorer (поиск скрытых процессов, handles, DLL).
4. Process Monitor (фильтрация событий файловой системы, реестра).
5. Autoruns (анализ автозагрузки, подозрительные записи).
6. TCPView (активные сетевые соединения, порты).
7. Встроенные средства Windows: systeminfo, netstat -anb, wmic, wevtutil.
8. Сбор DNS-кэша, ARP-таблицы, списка служб.

Раздел 2. Инструментальный анализ носителей и оперативной памяти

Лекция 6. ProDiscover – криминалистическая платформа

1. Назначение ProDiscover, отличия от EnCase, FTK, Autopsy.
2. Создание образа через ProDiscover (локально и удалённо).
3. Работа с образами: просмотр секторов, поиск по тексту/hex.
4. Анализ альтернативных потоков NTFS в ProDiscover.
5. Удалённый агент ProDiscover Agent для сбора с работающей системы.
6. Генерация отчётов (PDF, HTML, текст).
7. Экспорт подобранных файлов и фрагментов.

Лекция 7. Форензика оперативной памяти

1. Зачем делать дамп памяти: ключи шифрования, скрытые процессы, руткиты.
2. Методы захвата памяти (WinPmem, LiME, DumpIt, FTK Imager).

3. Влияние live-захвата на целостность памяти (атомарность дампа).
4. Структуры ядра Windows: EPROCESS, PEB, VAD tree, Handle table.
5. Особенности дампа Linux (/proc/kcore, fmem).
6. Проблемы разрыва связей между процессами и драйверами.
7. Обеспечение цепочки хранения для дампа памяти.

Лекция 8. Bulk Extractor – извлечение пассажирских данных

1. Принцип работы Bulk Extractor: сканирование без монтирования ФС.
2. Какие данные извлекает Bulk Extractor: email, URL, номера кредиток, пароли, SSID, телефонные номера.
3. Форматы входных данных: дамп памяти, образ диска, сетевой трафик (pcap).
4. Модули Bulk Extractor (base64, aes, net, xml, etc.).
5. Настройка фильтров для уменьшения ложных срабатываний.
6. Ограничения: не извлекает структурированные БД, не работает с шифрованием.
7. Сценарии применения при инциденте (утечка ПДн, фишинг).

Лекция 9. Volatility Framework – архитектура и базовые плагины

1. Архитектура Volatility 2 vs Volatility 3 (Python 3, символы).
2. Понятие профиля (OS, SP, архитектура, компиляция ядра).
3. Определение профиля через плагин imageinfo (Vol2) или windows.info (Vol3).
4. Базовые плагины: pslist, psscan, dlllist, hivelist, filescan.
5. Поиск скрытых процессов: разница между pslist (EPROCESS list) и psscan (сканирование памяти).
6. Деревья процессов, parent PID, некорректные завершения.
7. Работа с DLL процесса: поиск инжектированных библиотек.

Лекция 10. Volatility – работа с сетью, командной строкой и сокетами

1. Плагины для сети: netscan, sockscan, connscan (Windows), linux_net (Linux).
2. Восстановление открытых сокетов и соединений.
3. Поиск внедрённого кода: malfind, apihooks, ldrmodules.
4. Работа с реестром из дампа (hivelist, printkey).
5. Поиск инжектов в user-space и kernel-space.
6. Сценарии: обнаружение reverse shell, бэкдора, майнера.

Лекция 11. Scalpel и карательное восстановление файлов

1. Принцип работы Scalpel: конфигурационный файл (заголовки, хвосты).
2. Структура scalpel.conf: добавление собственных сигнатур.
3. Восстановление фрагментированных файлов (ограничения Scalpel).
4. Сравнение Scalpel, Foremost, Photorec.
5. Влияние размера блока сканирования и глубины поиска.
6. Ложные срабатывания из-за совпадения заголовков.
7. Автоматизация массового восстановления.

Раздел 3. Артефакты операционных систем, временные шкалы и экспертная деятельность

Лекция 12. Анализ журналов событий Windows

1. Формат .evtx, структура Event Log (каналы: Security, System, Application).
2. Ключевые Event ID для расследований: 4624 (успешный логин), 4625 (неудачный), 4688 (запуск процесса), 7045 (установка службы), 4656 (доступ к объекту).
3. Инструменты: Wevtutil, Get-WinEvent (PowerShell), LogParser, Event Viewer.
4. Корреляция временных штампов (UTC vs local).
5. Очистка логов и её обнаружение (Event ID 1102, 104).
6. Форензический анализ атак типа «pass-the-hash» по логам.
7. Права доступа к логам и их защита от изменения.

Лекция 13. Форензика реестра Windows

1. Структура кустов: SAM, SYSTEM, SOFTWARE, SECURITY, NTUSER.DAT, USRCLASS.DAT.
2. Ключи автозагрузки: Run, RunOnce, AppInit_DLLs, Shell, Userinit.
3. Артефакты USB: USBSTOR, SetupAPI (установка устройств, серийные номера).
4. MRU-списки (RecentDocs, ComDlg32, TypedURLs).
5. Сетевые артефакты: NetworkList, профили Wi-Fi (SSID, пароли).
6. Инструменты: RegRipper, Registry Explorer, Windows Registry Recovery.

7. Восстановление временных меток из реестра (последний запуск программы).

Лекция 14. Временные шкалы (timeline) в форензике

1. Понятие super-timeline: агрегация событий из MFT, логов, реестра, дампов памяти.
2. Инструменты: Log2Timeline (Plaso), Timesketch, timeline Explorer (SANS).
3. Формат выходных данных: bodyfile, CSV, Elasticsearch.
4. Фильтрация шума: исключение системных событий, фокусировка на пользователя.
5. Приоритизация событий по важности (Triage).
6. Визуализация временных линий для суда.
7. Примеры использования timeline для расследования утечки данных.

Лекция 15. Форензика ОС Linux

1. Структура системных логов: /var/log/syslog, auth.log, btmp, wtmp, lastlog.
2. Анализ истории команд: .bash_history, .zsh_history (временные метки, редактирование).
3. Поиск изменённых файлов: find / -mtime -n, использование debugfs/extundelete.
4. Артефакты запуска процессов через auditd (audit.log).
5. Анализ cron (/etc/crontab, пользовательские crontab).
6. Следы подключения по SSH: authorized_keys, known_hosts, логи sshd.
7. Восстановление удалённых файлов в ext4 (extundelete, debugfs).

Лекция 16. Мобильная форензика (базовые принципы)

1. Особенности мобильных устройств: постоянная связь, шифрование, блокировка экрана.
2. Методы извлечения: логический (ADB, iTunes backup), физический (JTAG, чип-офф), облачный.
3. Файловые системы: iOS (APFS, HFS+), Android (ext4, F2FS, crypto (FBE/FDE)).
4. Артефакты: SMS, MMS, звонки, геолокация (GPS, WiFi, сотовые вышки).
5. Приложения: WhatsApp, Telegram, Viber, Signal – где хранятся данные.
6. Правовые ограничения: ст. 13 УПК, 186.1 УК РФ, необходимость судебного решения.
7. Инструменты: Autopsy (модуль Android), MOBILedit, Cellebrite (обзорно).

Лекция 17. Отчётность эксперта и представление в суде

1. Структура заключения эксперта: вводная, исследовательская часть, выводы.
2. Стиль и язык: недопустимость субъективных оценок («вероятно», «скорее всего»).
3. Иллюстрации: скриншоты, timeline, таблицы, хэш-суммы.
4. Оформление ссылок на методики и ПО (версии, параметры).
5. Подготовка к перекрёстному допросу (moot court): слабые места заключения.
6. Понятие «экспертная ошибка» и как её избежать.
7. Примеры заключений из реальных дел.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Создание криминалистически корректного образа диска	2
2	1	Оформление документации	2
3	1	Анализ файловой системы в Sleuth Kit	2
4	1	Восстановление удалённых файлов Autopsy	2
5	1	Sysinternals – анализ подозрительной активности	2
6	2	ProDiscover – базовый анализ образа	2
7	2	Сбор данных – создание дампа памяти	2
8	2	Работа с дампами памяти в Bulk Extractor	2
9	2	Анализ дампа памяти с использованием Volatility	2
10	2	Volatility – сетевые артефакты и инжекты	2
11	2	Восстановление удаленных данных с образа. Scalpel	2
12	3	Анализ логов событий Windows	2
13	3	Анализ артефактов реестра	2
14	3	Создание временной шкалы с Plaso	2
15	3	Анализ Linux-системы после инцидента	2
16	3	Извлечение артефактов из образа Android	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
17	3	Формирование полного экспертного заключения	2
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Шевелева, К. В. Криминалистические средства и методы собирания доказательств : учебное пособие / К. В. Шевелева. — Москва : РТУ МИРЭА, 2025. — 96 с. — ISBN 978-5-7339-2729-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/513044 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей.

2. Веселова, С. В. Цифровая обработка изображений : учебное пособие / С. В. Веселова, Е. В. Константинова, И. В. Александрова. — Санкт-Петербург : СПбГИКиТ, 2021. — 283 с. — ISBN 978-5-94760-493-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/415985 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1. Ермакова, А. Н. Цифровой след: формирование и управляемость в экономике данных : монография / А. Н. Ермакова. — Ставрополь : СтГАУ, 2024. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/510158 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей.

2. Колесникова, Н. С. Значение судебного эксперта в процессе формирования криминалистически значимой информации: проблемы и решения : учебное пособие / Н. С. Колесникова. — Белгород : НИУ БелГУ, 2021. — 64 с. — ISBN 978-5-9571-3131-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/329255 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

1. Закон и право - https://eivis.ru/browse/publication/81027/udb/12/ закон-и-право
2. Защита информации. Инсайд - https://eivis.ru/browse/publication/122426/udb/12/ защита-информации-инсайд

5.4 Интернет-ресурсы

https://www.pvsm.ru/ 70+ бесплатных инструментов для компьютерной криминалистики
https://codeib.ru/ КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ Autopsy User's Guide (v4.21.0)
http://sleuthkit.org/autopsy/docs/user-docs/4.22.0/workflow_page.html Autopsy Workflow (v4.22.0)
https://volatility3.readthedocs.io/en/v1.0.1/using-as-a-library.html Using Volatility 3 as a Library
https://subscription-non-live.prod.packtpub.com/book/security/9781788625005/6/ch06lvl1sec44/bulk-extractor Digital Forensics with Kali Linux

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru
5. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный персональными компьютерами с установленным программным обеспечением.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.